Communications Security Establishment Commissioner

Annual Report

2000 ↓ 2001

Canada

Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station 'B'
Ottawa, Ontario
K1P 5R5

Tel: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 2001
ISBN 0-662-65817-5
Cat. No. D95-2001

101-04780/

Communications Security Establishment Commissioner

The Honourable Claude Bisson, O.C.

CANADA

Commissaire du Centre de la sécurité des télécommunications

L'honorable Claude Bisson, O.C.

May 2001

The Honourable Arthur C. Eggleton, P.C.
Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Mr. Eggleton:

Pursuant to paragraph (g) of Order in Council P.C. 1999-1048 re-appointing me Communications Security Establishment Commissioner, I am pleased to submit to you my 2000-2001 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Claude Bisson

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: *(613)* 992-4096

TABLE OF CONTENTS

Introduction 1

CSE Today 2

- Mandate 2
- Signals Intelligence 2
- Information Technology Security 3
- Relationships with allies 4
- Controls on CSE's activities 4
- CSE's recent contributions 5

Evolution of CSE 6

- The pressures for change 6
- CSE's strategic plan 7

Reviewing CSE 8

- The Commissioner's role 8
- 2000-2001 activities 9
  - Foreign intelligence product 9
  - Information management 10
  - Policy authority 11
  - Other activities 11
- 2000-2001 findings 12
- Office staff and budget 12

Looking Ahead 13

- Safeguarding the privacy of Canadians 13

Annex A: Commissioner's Mandate 15

Annex B: Classified Reports, 1996-2001 19

INTRODUCTION

In the five-year period since my appointment, I have observed the emergence of complex global communications technologies, together with evolving political, social and economic realities. This environment has led to the identification of new threats to Canada's security, defence and national interests and a pressing need for the Government of Canada to determine how to counter these threats.

During this same period, the Communications Security Establishment (CSE) has sought to maintain its ability to meet the government's evolving foreign intelligence priorities and to protect the integrity of its communications and information systems.

I believe that a failure to maintain CSE's capabilities would have serious implications for Canada's national interests. For example, if CSE were unable to report on the activities and intentions of foreign states and persons, Canada's political and economic well-being would be at risk. Furthermore, if CSE could no longer protect government information systems and assets, the government's efforts would be crippled in the areas of electronic service delivery and e-commerce, ultimately to the detriment of Canada's economic competitiveness.

Technological advancements will certainly continue and may even accelerate. CSE's senior management has informed me that they are convinced CSE must refocus its efforts to meet its responsibilities to government, or risk lagging behind. As a result, in consultation with its stakeholders, CSE has adopted a renewed strategic approach to its mandate.

This is the environment in which I continue to examine CSE's activities to determine their compliance with the laws of Canada and to assess CSE's efforts to safeguard the privacy of Canadians.

As in my previous annual reports, I will look back in this 2000-2001 Annual Report on CSE's performance over the past year.

CSE TODAY

Mandate

CSE, an agency of the Department of National Defence, assists the Government of Canada in two distinct but related areas:

- It provides the government with foreign intelligence by collecting, analyzing and reporting on foreign radio, radar and other electronic signals (signals intelligence, or SIGINT).
- It helps ensure the Canadian government's telecommunications and information technologies are secure from interception, disruption, manipulation or sabotage (information technology security, or ITS).

The Minister of National Defence is fully accountable to Parliament for CSE. He is supported by two senior officials — the Deputy Minister of National Defence, for financial and administrative matters, and the Deputy Clerk of the Privy Council, Counsel and Security and Intelligence Coordinator, for policy and operational matters.

Signals Intelligence

CSE's SIGINT program is guided by the foreign intelligence priorities established annually by the Meeting of Ministers on Security and Intelligence, chaired by the Prime Minister.

To fulfill its SIGINT mandate, CSE acquires various modes of foreign communications signals. The collection and processing of these signals involve highly sophisticated and complex technologies. Processing often includes the decryption and translation of encrypted communications to make them intelligible.

Encryption falls within the science known as cryptology, which uses mathematical algorithms to hide or disguise communications.

I have learned from CSE that advancements in global transmissions present continuing challenges to the collection and processing of foreign signals. The tremendous volume of communications signals produced every day, together with the increased use and public availability of encryption software, has added to these challenges.

As a result, CSE has dedicated additional resources to the research and development of techniques to acquire and process communications, so that the government can be kept apprised of threats to Canada's interests. To accomplish this, CSE relies on the capabilities of a cross-section of skilled workers, including computer scientists, mathematicians and linguists. To produce intelligence reports it also needs analysts knowledgeable in such matters as international political, economic and military affairs, terrorism, and transnational crime. These reports are the vehicle through which CSE communicates foreign intelligence information to its Government of Canada clients. More than 100,000 SIGINT reports are made available to CSE's readership every year.

Information Technology Security

The development and application of new technologies in recent years has transformed the focus and complexity of the activities undertaken by CSE to protect government communications and communications systems, the mandate of its Information Security Technology (ITS) program.

Until fairly recently, computer hardware, software and networks were not widely available and had limited application. Today, however, the computer is a fully established means of daily

communication among people. It drives many of the technologies that make up Canada's critical information infrastructure.

This communications environment has introduced new vulnerabilities to government information systems that require alternative solutions to counter threats to security and privacy.

The government looks to CSE to protect information stored or transmitted on its computer systems while, at the same time, departments and agencies work toward making a multiplicity of services available to the public on-line. Meanwhile, by law, personal information about Canadians must be protected, despite the fact that government computer systems are increasingly interconnected and vulnerable to disruption and to such threats as denials of service.

Relationships with allies

Canada benefits from longstanding arrangements between CSE and its counterparts in the United States, the United Kingdom, Australia, and New Zealand. These arrangements, which were formalized after the Second World War and maintained during the Cold War, allow for the exchange of signals intelligence, technology and information about sources and techniques of shared interest.

As part of my ongoing review of CSE's activities, I am satisfied that CSE does not use its partners to circumvent the laws of Canada, nor does it provide partners with communications they could not legally collect for themselves.

Controls on CSE's activities

Based upon my review activities to date, I have observed that CSE's activities are guided by law and policy and the government's priorities, not by its technical capabilities. In addition to my own reviews, CSE is also subject to the independent

scrutiny of many, including the courts, the Privacy Commissioner, the Information Commissioner, the Canadian Human Rights Commission, and the Auditor General of Canada.

Today's global communications networks generate an inordinate volume of information with which CSE must contend. This volume is in and of itself a control. In practical terms, CSE must stay focused on its mandate in order to meet the foreign intelligence priorities it is given.

CSE's recent contributions

The government uses CSE's intelligence reporting to further Canada's economic and political interests in its relationships with foreign states.

The Canadian Forces enter peacekeeping operations abroad with an enhanced understanding of the situation on the ground as a result of CSE's contributions.

CSE provides its government clients responsible for protecting public safety with information derived from foreign intelligence that contributes to efforts directed at countering terrorism, weapons proliferation, drug smuggling, illegal migration, and transnational crime. More recently, CSE has begun to provide these same clients with technical assistance.

CSE is working closely with the Canadian Forces Information Operations Group (CFIOG) to enhance support to Canadian military operations, with direct service now provided by CFIOG. (CFIOG was created in April 1998 from a consolidation of various National Defence elements, including the Canadian Forces Supplementary Radio Systems. It provides a focal point for Information Operations).

Through its ITS program, CSE continues to encourage and support Canadian firms in the development of new security products.

Additionally, CSE has an ongoing relationship with several government departments and agencies and assists them in assessing their ITS needs as they migrate toward on-line service delivery.

CSE provided senior level expertise to the government's Critical Infrastructure Protection Task Force. Created in April 2000, the Task Force recommended what the federal government should do to protect that part of Canada's infrastructure that is critical to the health, safety, security, and economic well-being of Canadians.

EVOLUTION OF CSE

The pressures for change

CSE must contend with the revolutionary pace of technological change. The foundation of its activities is technology, which affects CSE, like its partners, in several ways:

- The channels through which foreign communications travel are multiplying. The new wireless, fibre optic and Internet communications technologies continue to advance, requiring CSE's computer scientists and engineers to expand and upgrade their knowledge base constantly.
- The targets of foreign intelligence collection activities, including terrorist groups, now have easy access to the sophisticated products of a multi-trillion dollar telecommunications industry, including digital encryption technology, available as freeware on the World Wide Web, making it difficult if not impossible to decipher their communications.
- Increasingly, vast amounts of information are moving through new channels of communication, making it highly labour-intensive for CSE to identify useful information.
- Canadian government departments and agencies are also using new modes of communication that interconnect with computer systems that contain

sensitive information or control critical infrastructure. They look to CSE's ITS experts for advice to protect their communications networks and computer systems.

- The number of attacks on government networks and systems is growing. A September 2000 study on threats to federal Internet sites estimated that a typical site is subject to 10 or more threat incidents each week. Moreover, the frequency of foreign attacks on US systems that originate or pass through Canada is becoming an issue.
- The government's new Office of Critical Infrastructure Protection and Emergency Preparedness, announced in February 2001 and charged with developing and implementing a comprehensive approach to protecting Canada's critical infrastructure, will look to CSE for technical support.

CSE's strategic plan

During the year under review, CSE embarked upon an important strategic exercise to identify alternative approaches to delivering its mandate.

As a starting point, CSE defined its vision: "to be the agency that masters the global information network to enhance Canada's safety and prosperity". In so doing, CSE has effectively returned to its roots with the recognition that its core strength is its ability to understand and protect communications and communications systems. CSE's ability to exploit these systems to provide foreign intelligence flows from this core strength.

In support of its vision, CSE aims to become a centre of excellence that develops and applies its technical expertise and understanding of global communications networks and helps Canada meet its critical information needs.

CSE has adopted three strategic goals for the next 10 years:

- to be the acknowledged governmental centre of excellence in understanding and addressing the capacities of the global network
- to protect and enable the Canadian information infrastructure
- to modernize CSE services, products and delivery.

As a first step, CSE has strengthened the linkage between its SIGINT and ITS programs. Although their activities are related, they have traditionally operated at arm's length from each other. To achieve its strategic goals, CSE intends to benefit from the synergies created by drawing the two programs closer. By exploring the vulnerabilities of communications and information systems together, SIGINT and ITS experts now pool their knowledge to identify threats to Canadian systems as well as opportunities for foreign intelligence collection.

In June 2000, the Chief of CSE briefed me on this topic. Subsequently, my office has discussed the strategy in detail with CSE's senior management. I do not believe this approach will change how I review CSE's activities in any fundamental way, since my focus will remain on their lawfulness. In the meantime, I have expressed my support of this undertaking.

REVIEWING CSE

The Commissioner's role

My mandate to review the activities of CSE and to report to the Minister of National Defence is contained in an Order in Council (see Annex A).

Each year, my office identifies areas within CSE's operations where, at first view, questions of lawfulness might be presumed. Under my authority, my office then conducts systematic reviews of these

operations. I pass the results of these reviews to the Minister of National Defence in the form of classified reports. The fact that I have issued a classified report is not an indication that I have uncovered an incident of unlawfulness. Rather, it is an indication that the report contains sensitive information that requires classified handling.

The effort that goes into researching and preparing my reports to the Minister accounts for the bulk of the work of my office and gives me a detailed understanding of various aspects of CSE's operations.

I have reviewed CSE's authorities to collect foreign intelligence on behalf of the Government of Canada and its mandate to protect the security of the government's information technology. On an ongoing basis, I examine CSE's policies, directives and actual practices to ensure they contribute to lawfulness and to protecting Canadians' privacy.

Among other issues, my reviews have looked at how CSE provides intelligence reports to its clients, and the receipt of intelligence from its Second Party partners. I regularly monitor CSE's operational activities, as well as circumstances that have led to internal security investigations.

Annex B contains a list of the classified reports I have passed to the Minister since my appointment in 1996.

2000-2001 activities

Foreign intelligence product

During the past year, I continued to review CSE's activities as they relate to the intelligence cycle and the handling and production of intelligence product. As I outlined in my last annual report, CSE conducts daily reviews of the raw traffic it receives from multiple sources and assesses its foreign intelligence value against the government's

priorities. CSE then passes the results to its government clients in the form of intelligence product.

This past year, I reviewed the policies and handling practices associated with CSE's receipt and retention of foreign intelligence traffic. I examined how CSE identifies issues of intelligence interest within the raw traffic it receives and the practices associated with its retention and subsequent dissemination in the form of intelligence reporting. And, as is my practice, I reviewed CSE's policies and practices, within this cycle of activities, that deal specifically with safeguarding the privacy of Canadians.

Information management

I also reviewed CSE's information management policies in light of the National Archives of Canada Act and Treasury Board policy and guidelines related to the management of information holdings.

Government departments and agencies are required to establish Records Disposition Authorities for their operational and administrative holdings. These Authorities grant permission to departments and agencies to dispose of certain holdings and require them to forward to the National Archives other holdings identified to be of archival interest, for preservation.

I observed that these Authorities do not constitute a requirement to destroy records, nor do they provide direction regarding the timing of records destruction. Moreover, they do not provide or authorize records retention periods. Retention and disposal periods are determined by the designated Minister of the institution and must, of course, conform to any other applicable legislation.

I was satisfied that CSE's policies conform with existing law and policy requirements related to the management of government information holdings. I recommended, however, that CSE give priority to completing its retention and disposal schedules.

Policy authority

In my 1998-99 Annual Report, I indicated my intention to examine the new framework for policy authority, accountability and coordination that CSE had recently adopted. Of particular interest to me were two of the objectives of the framework: to identify the appropriate level of authority for various policies; and to provide a desirable level of operational flexibility in support of day-to-day activities.

During the past year, I reviewed the new framework and found it to be well conceived and sound. It will take time, however, to convert all CSE policy to the framework. While some policy gaps remain, CSE has policies for its major requirements, and the new system should address my earlier concerns about having policy in the right place and signed off at the right level.

During the year under review, I was pleased to learn that officials had opened discussions on having cornerstone internal policies issued to CSE as Ministerial direction. I applaud this initiative, because it will strengthen the accountability linkages between CSE and the Minister of National Defence, who is responsible for CSE in Parliament.

Other activities

My mandate authorizes me to investigate complaints by Canadians or permanent residents of Canada about CSE activities. While there were informal inquiries during 2000-2001, none led to a formal complaint.

During the past year, my office has maintained its informal contacts within the security and intelligence community. We were particularly pleased to receive the Inspector General of South Africa during his autumn 2000 tour of North America. I look forward to renewing acquaintances with my counterparts from other countries at the upcoming conference of review agencies in Washington in October 2001.

2000-2001 findings

I am satisfied that during the period under review, CSE acted lawfully in the performance of its mandated activities and did not target the communications of Canadian citizens or permanent residents. I make this statement on the basis of the thorough review of CSE's activities conducted during the year.

My mandate requires me to inform the Minister of National Defence and the Attorney General of Canada of any CSE activity that I believe may not be in compliance with the law. To date, I have not been required to do so. CSE is aware of its boundaries, receives legal advice from counsel appointed to CSE by the Department of Justice, and has policies and procedures in place to promote lawfulness. These measures have proven to be effective.

Office staff and budget

During the 2000-2001 fiscal year, my budget allocation was $648,800. I can report that actual expenses incurred were well within budget.

My office continues to consist of two full-time employees and a number of subject-matter experts whom I employ on contract. At present, there are five people performing specialized work under this arrangement, all of whom have the required security clearances. This provides me with both continuity and flexibility to obtain the expertise I require to review CSE's activities effectively.

LOOKING AHEAD

Safeguarding the privacy of Canadians

As I have previously observed, CSE's foreign intelligence collection technology must constantly progress to keep pace with advances in communications technology. Despite the efficiencies inherent in new technologies, CSE is still likely to receive inadvertently some small amount of Canadian communications. Moreover, each new collection system or technique that comes on stream seems to bring with it this potential. However, CSE is well aware that it must continually upgrade its capabilities to screen out Canadian communications or risk acting unlawfully if it does not make every effort to do so.

In this regard, I have informed CSE that, in addition to my other review activities, I will be seeking assurance that it is availing itself of all emerging technologies to ensure that the privacy of Canadians is safeguarded.

CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

P.C. 1999-1048
June 8, 1999

His Excellency the Governor General in Council, on the recommendation of the Minister of National Defence, pursuant to Part II of the *Inquiries Act*, hereby authorizes the Minister of National Defence (in this order referred to as "the Minister")

(*a*) to re-appoint the Honourable Claude Bisson of Montreal, Quebec, for a period of three years, as a commissioner ("the Commissioner") to review the activities of the Communications Security Establishment ("CSE") for the purpose of determining whether those activities are in compliance with the law;

(*b*) to authorize the Commissioner to commence that review on his own initiative or at the request of the Minister;

(*c*) to authorize the Commissioner to investigate any complaint, concerning the lawfulness of CSE activities, made by any individual who is a Canadian citizen or a permanent resident of Canada;

(*d*) to authorize the Commissioner not to investigate complaints for which, in the Commissioner's opinion, other avenues of redress are established by statute;

(*e*) to specifically authorize the Commissioner to inform any complainant of the results of his investigation, ensuring that no classified information is disclosed to the complainant;

(*f*) to direct the Commissioner to inform the Minister and the Attorney General of Canada of any CSE activity that the Commissioner believes may not be in compliance with the law;

.../2

(*g*) to direct the Commissioner to submit to the Minister, once each year and in both official languages, a report on the Commissioner's activities and findings that are not classified, which report the Minister will table in Parliament;

(*h*) to authorize the Commissioner, at any time the Commissioner considers it advisable, to submit a report containing classified information to the Minister;

(*i*) to direct the Commissioner, before submitting any report to the Minister, to consult with the Deputy Secretary to the Cabinet (Security and Intelligence) at the Privy Council Office for the purpose of ensuring compliance with all security requirements and the preservation of the secrecy of sources of security and intelligence information and of the security of information provided to Canada in confidence by other nations;

(*j*) to direct the Commissioner and all persons engaged on his behalf take an oath of secrecy and comply with all applicable government security requirements;

(*k*) to authorize the Commissioner to engage the services of any staff, advisors and counsel that he considers necessary to assist him in the performance of his duties and functions at such rates of remuneration and reimbursement as may be approved by the Treasury Board;

.../3

(l) to fix the remuneration of the Commissioner at the per diem rate set out in the annexed schedule, which rate is within the range of $400 to $500; and

(m) to authorize that the Commissioner be paid reasonable travel and living expenses incurred by him in the performance of his duties and functions while absent from his ordinary place of residence, in accordance with Treasury Board travel directives;

effective June 19, 1999.

CERTIFIED TO BE A TRUE COPY-COPIE CERTIFIÉE CONFORME

CLERK OF THE PRIVY COUNCIL-LE GREFFIER DU CONSEIL PRIVÉ

Classified Reports, 1996-2001

Classified Report to the Minister - March 3, 1997 (TOP SECRET)

Classified Report to the Minister
- Operational Policies with Lawfulness Implications - February 6, 1998 - (SECRET)

Classified Report to the Minister
- CSE's Activities under *** - March 5, 1998 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
- Internal Investigations and Complaints - March 10, 1998 (SECRET)

Classified Report to the Minister
- CSE's activities under *** - December 10, 1998 (TOP SECRET/CEO)

Classified Report to the Minister
- On controlling communications security (COMSEC) material - May 6, 1999 (TOP SECRET)

Classified Report to the Minister
- How We Test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) - June 14, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
- A Study of the *** Collection Program - November 19, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
- On *** - December 8, 1999 (TOP SECRET - COMINT)

Classified Report to the Minister
- Study of the *** Reporting Process - an overview (Phase I) - December 8, 1999 (SECRET/CEO)

Classified Report to the Minister
- A Study of Selection and *** - an overview - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- CSE's Operational Support Activities Under *** - follow-up - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- Internal Investigations and Complaints - follow-up - May 10, 2000 (SECRET)

Classified Report to the Minister
- On findings of an external review of CSE's ITS Program - June 15, 2000 (SECRET)

Classified Report to the Minister
- CSE's Policy System Review - September 14, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase II *** - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase III *** - April 6, 2001 (SECRET/CEO)

Commissaire
du Centre
de la sécurité
des télécommunications

Rapport annuel

2000
↓
2001

Canada

Bureau du Commissaire du Centre de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Téléc. : (613) 992-4096

© Ministre des Travaux publics et des Services gouvernementaux Canada 2001
ISBN 0-662-65817-5
N° de cat. D95-2001

Communications Security Establishment Commissioner

CANADA

Commissaire du Centre de la sécurité des télécommunications

The Honourable Claude Bisson, O.C.

L'honorable Claude Bisson, O.C.

Mai 2001

L'honorable Arthur C. Eggleton, C.P.
Ministre de la Défense nationale
Édifice Mgén G.R. Pearkes, 13e étage
101, promenade Colonel By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément à l'alinéa g) du décret C.P. 1999-1048 prévoyant le renouvellement de ma nomination au poste de commissaire du Centre de la sécurité des télécommunications, j'ai le plaisir de vous soumettre mon rapport annuel pour l'année 2000-2001, qui fait état de mes activités et constatations, pour présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Claude Bisson

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE DES MATIÈRES

Introduction 1

Le CST aujourd'hui 2
- Mandat 2
- Le renseignement électromagnétique 3
- La sécurite des technologies de l'information 4
- Relations avec les alliés 4
- Contrôle des activités du CST 5
- Contributions récentes du CST 5

Évolution du CST 7
- Des pressions dans le sens du changement 7
- Le plan stratégique du CST 8

Examen du CST 9
- Le rôle du commissaire 9
- Activités de l'année 2000-2001 11
  - Produits du renseignement sur l'étranger 11
  - Gestion de l'information 11
  - Pouvoirs en matière de politiques 12
  - Autres activités 13
- Constatations faites en 2000-2001 13
- Personnel et budget 14

Coup d'œil sur l'avenir 14
- Sauvegarder la vie privée des Canadiens 14

Annexe A : Mandat du commissaire 15

Annexe B : Rapports classifiés, 1996-2001 19

INTRODUCTION

Au cours des cinq années écoulées depuis ma première nomination, j'ai vu naître des technologies de communication mondiale complexes, parallèlement à l'évolution des réalités politiques, sociales et économiques. Cette situation a mis en évidence de nouvelles menaces à la sécurité, à la défense et aux intérêts nationaux du Canada et fait ressortir le besoin pressant pour le gouvernement du Canada de déterminer comment parer à ces menaces.

Au cours de la même période, le Centre de la sécurité des télécommunications (CST) s'est efforcé d'entretenir sa capacité de répondre aux priorités du gouvernement en matière de renseignement sur l'étranger à mesure de leur évolution, et de protéger l'intégrité de ses systèmes de communication et d'information.

Je suis convaincu que, si les capacités du CST n'étaient pas entretenues comme il convient, les intérêts nationaux du Canada seraient gravement compromis. Par exemple, si le CST n'était pas en mesure de faire rapport sur les activités et les intentions d'États et d'individus étrangers, le bien-être politique et économique du Canada serait menacé. De plus, si le CST ne pouvait plus protéger les systèmes d'information et les fonds de renseignements du gouvernement, les efforts de celui-ci seraient paralysés dans les domaines de la prestation électronique des services et du commerce électronique, ce qui nuirait finalement à la compétitivité économique du Canada.

Les progrès technologiques se poursuivront certainement et pourraient même s'accélérer. La haute direction du CST m'a informé de sa conviction que celui-ci doit réorienter ses efforts pour s'acquitter de ses responsabilités envers le gouvernement, faute de quoi il risque d'être à la traîne. En conséquence, le CST a adopté, en

consultation avec les parties intéressées par son activité, une nouvelle approche stratégique relativement à son mandat.

Tel est le contexte dans lequel je continue d'examiner les activités du CST, afin de déterminer leur conformité aux lois du Canada, et d'évaluer les efforts qu'il déploie pour sauvegarder la vie privée des Canadiens.

Comme je l'ai fait les années précédentes, j'examine dans le présent rapport la façon dont le CST s'est acquitté de son mandat au cours de l'année écoulée.

LE CST AUJOURD'HUI

Le CST est un organisme du ministère de la Défense nationale, qui aide le gouvernement dans deux domaines distincts, mais liés entre eux :

Mandat

- Il fournit au gouvernement des renseignements sur l'étranger en recueillant et analysant les signaux radio, radar et autres signaux électroniques de pays étrangers et en lui communiquant des rapports à ce sujet (renseignement électromagnétique ou SIGINT).
- Il contribue à faire en sorte que les télécommunications et les technologies de l'information du gouvernement canadien soient protégées contre l'interception, la perturbation, la manipulation et le sabotage (sécurité des technologies de l'information ou STI).

Le ministre de la Défense nationale est pleinement comptable du CST devant le Parlement. Il est soutenu à cet égard par deux hauts fonctionnaires, soit le sous-ministre de la Défense nationale, pour les questions financières et administratives, et le sous-greffier du Conseil privé, conseiller juridique et coordonnateur de la sécurité et du renseignement, pour les affaires stratégiques et opérationnelles.

Le renseignement électromagnétique

Le programme de SIGINT du CST est guidé par les priorités en matière de renseignement sur l'étranger établies annuellement par la réunion des ministres sur la sécurité et le renseignement, que préside le Premier ministre.

Pour s'acquitter de son mandat en matière de SIGINT, le CST recueille les signaux émis par divers modes de communication de pays étrangers. La collecte et le traitement de ces signaux font intervenir des technologies très sophistiquées et très complexes. Le traitement comprend souvent le déchiffrage et la traduction de communications chiffrées pour les rendre intelligibles. Le chiffrement relève de la cryptologie, science qui utilise des algorithmes mathématiques pour dissimuler ou déguiser des communications.

Le CST m'a informé que les progrès accomplis dans le domaine des transmissions mondiales présentent des défis permanents à la collecte et au traitement des signaux étrangers. Les quantités énormes de signaux de communications produits quotidiennement, alliées au recours accru aux logiciels de chiffrement et à la disponibilité publique de ceux-ci, ne font qu'ajouter à ces défis.

En conséquence, le CST a consacré des ressources additionnelles à la recherche et au développement de techniques de collecte et de traitement des communications, afin que le gouvernement puisse être tenu au courant des menaces visant les intérêts du Canada. À cette fin, le CST fait appel à un ensemble de spécialistes, dont des informaticiens, des mathématiciens et des linguistes. Il a en outre besoin d'analystes du renseignement bien au fait de questions comme les affaires politiques, économiques et militaires internationales, le terrorisme et la criminalité transnationale, afin de produire des rapports de renseignement. Ces rapports sont le moyen par lequel le CST communique l'information relative au

renseignement sur l'étranger à ses clients du gouvernement du Canada. Plus de 100 000 rapports de SIGINT sont mis à la disposition de ceux-ci chaque année.

La sécurité des technologies de l'information

Ces dernières années, le développement et la mise en œuvre de nouvelles technologies ont transformé l'orientation et la complexité des activités entreprises par le CST, dans le cadre de son programme de STI, afin de protéger les communications et les systèmes de communication du gouvernement.

Jusqu'à récemment, le matériel informatique, les logiciels et les réseaux n'étaient pas encore très répandus et n'avaient qu'une application limitée. À l'heure actuelle, cependant, l'ordinateur s'est imposé comme moyen de communication entre les gens et il est à l'origine de nombreuses technologies qui forment l'infrastructure canadienne en matière d'information critique.

Ce contexte a fait apparaître, dans les systèmes d'information du gouvernement, de nouvelles vulnérabilités qui exigent des solutions nouvelles permettant de parer aux menaces à la sécurité et à la vie privée.

Le gouvernement compte sur le CST pour protéger l'information stockée dans ses systèmes informatiques ou transmise par ceux-ci, tandis que divers ministères et organismes s'appliquent à mettre une multiplicité de services en ligne à la disposition du public. Parallèlement, la loi exige que les renseignements personnels au sujet des Canadiens soient protégés, alors que les systèmes informatiques du gouvernement sont de plus en plus interreliés et vulnérables aux perturbations et à des menaces comme les dénis de service.

Relations avec les alliés

Le Canada profite d'arrangements de longue date conclus entre le CST et ses homologues des États-Unis, du Royaume-Uni, de l'Australie et de la

Nouvelle-Zélande. Ces arrangements, qui ont été officialisés après la Deuxième Guerre mondiale et maintenus durant la guerre froide, permettent l'échange de renseignements électromagnétiques, de technologies et d'information au sujet de sources et de techniques d'intérêt commun.

Dans le cadre de mon travail régulier d'examen des activités du CST, je peux affirmer que celui-ci ne se sert pas de ses partenaires pour contourner les lois du Canada, et qu'il ne leur fournit pas de communications qu'ils ne pourraient pas recueillir légalement eux-mêmes.

Contrôle des activités du CST

En me fondant sur les travaux d'examen que j'ai effectués jusqu'ici, je constate que les activités du CST sont guidées par la loi, par ses principes généraux et par les priorités du gouvernement, et non par les moyens techniques dont il dispose. En plus de mes propres examens, le CST est par ailleurs assujetti à l'examen indépendant de nombreuses instances, notamment les tribunaux, le commissaire à la protection de la vie privée, le commissaire à l'information, la Commission canadienne des droits de la personne et le vérificateur général du Canada.

Les réseaux actuels de communication mondiale génèrent une quantité excessive d'information à laquelle le CST doit faire face. Cette quantité est en soi un contrôle. D'un point de vue pratique, le CST doit rester concentré sur son mandat s'il veut répondre aux priorités qui lui sont assignées en matière de renseignement sur l'étranger.

Contributions récentes du CST

Le gouvernement utilise les rapports de renseignement du CST pour favoriser les intérêts économiques et politiques du Canada dans ses relations avec les États étrangers.

Les forces canadiennes qui s'engagent dans des opérations de maintien de la paix à l'étranger comprennent mieux la situation sur le terrain grâce aux renseignements fournis par le CST.

Le CST fournit à ses clients du gouvernement chargés de protéger la sûreté publique de l'information tirée des renseignements sur l'étranger, qui contribuent aux efforts de lutte contre le terrorisme, la prolifération des armes, le trafic de la drogue, la migration illégale et la criminalité transnationale. Plus récemment, il a commencé à fournir aux mêmes organismes une assistance technique.

Le CST collabore étroitement avec le Groupe des opérations d'information des Forces canadiennes (GOIFC), afin d'améliorer l'appui qu'offre directement le Groupe dans le cadre des opérations militaires du Canada. (Créé en avril 1998, le GOIFC regroupe divers éléments du ministère de la Défense nationale, notamment le Réseau radio supplémentaire des Forces canadiennes. Il constitue un centre névralgique pour les opérations d'information.)

Dans le cadre de son programme de STI, le CST continue d'encourager et d'aider des entreprises canadiennes à mettre au point de nouveaux produits de sécurité. Il entretient par ailleurs des relations suivies avec plusieurs ministères et organismes et les aide à évaluer leurs besoins en matière de STI à mesure qu'ils s'orientent vers la prestation de services en ligne.

Le CST a fourni une expertise de niveau supérieur au Groupe de travail du gouvernement sur la protection des infrastructures essentielles. Ce groupe de travail, créé en avril 2000, a recommandé les mesures que le gouvernement fédéral devrait prendre pour protéger la partie de l'infrastructure du Canada qui est essentielle à la santé, à la sûreté, à la sécurité et au bien-être économique des Canadiens.

ÉVOLUTION DU CST

Des pressions dans le sens du changement

Le CST doit composer avec le rythme révolutionnaire de l'évolution technologique. Le fondement de ses activités est la technologie, qui touche l'organisme, et ses partenaires, de plusieurs façons :

- Les canaux de transmission des communications étrangères se multiplient. Les nouvelles techniques de communication sans fil, par fibres optiques et par Internet continuent de progresser, ce qui oblige les informaticiens et les ingénieurs du CST à accroître et étendre constamment leurs connaissances.
- Les cibles des activités de collecte de renseignements sur l'étranger, dont les groupes terroristes, ont maintenant facilement accès aux produits sophistiqués d'une industrie des télécommunications représentant plusieurs billions de dollars, y compris la technologie de chiffrement numérique, qui est disponible à titre de logiciel public sur Internet, de sorte qu'il est difficile, sinon impossible, de déchiffrer leurs communications.
- De plus en plus, des quantités énormes d'information sont acheminées sur les nouveaux canaux de communication, de sorte que le CST doit affecter un personnel très nombreux pour déceler les renseignements utiles.
- Les ministères et organismes du gouvernement canadien emploient aussi de nouveaux modes de communication interconnectés avec des systèmes informatiques contenant des renseignements de nature délicate, ou qui contrôlent des infrastructures essentielles. Ils comptent sur les experts du CST en matière de STI pour leur donner des conseils afin de protéger leurs réseaux de communication et leurs systèmes informatiques.

- Le nombre d'attaques dirigées contre les réseaux et les systèmes gouvernementaux est en hausse. Selon une estimation contenue dans une étude effectuée en septembre 2000 sur les menaces visant les sites Internet fédéraux, un site typique fait l'objet de 10 incidents de menace ou plus chaque semaine. De plus, la fréquence des attaques contre les systèmes américains provenant du Canada ou passant par notre pays commence à poser problème.
- Le nouveau Bureau de la protection de l'infrastructure essentielle et de la planification d'urgence, dont la création a été annoncée par le gouvernement en février 2001 et qui est chargé d'élaborer et de mettre en œuvre un plan complet de protection de l'infrastructure essentielle du Canada, comptera sur le soutien technique du CST.

Le plan stratégique du CST

Pendant l'année examinée, le CST a entrepris un important travail stratégique afin de trouver de nouvelles manières d'exécuter son mandat.

À cette fin, il a d'abord défini sa vision, soit : « être l'organisme qui maîtrise le réseau mondial d'information afin d'accroître la sécurité et la prospérité du Canada ». Ce faisant, le CST est effectivement retourné à ses origines en reconnaissant que sa force de base réside dans sa capacité de comprendre et de protéger les communications et les systèmes de communication. Sa capacité d'exploiter ces systèmes pour fournir des renseignements sur l'étranger découle de cette force de base.

Pour soutenir sa vision, le CST vise à devenir un centre d'excellence qui développera et appliquera ses compétences techniques et sa connaissance des réseaux de communication mondiale, et il compte aider le Canada à répondre à ses besoins d'information essentiels.

Le CST s'est fixé trois buts stratégiques pour les 10 prochaines années :

- être reconnu comme le centre d'excellence du gouvernement pour ce qui est de l'analyse et de l'exploitation des capacités du réseau mondial;
- protéger l'infrastructure d'information du Canada et veiller à son bon fonctionnement;
- moderniser les produits et les services du CST ainsi que leur mode de prestation.

Dans un premier temps, le CST a renforcé les liens entre ses programmes de SIGINT et de STI. Même si leurs activités ont un rapport entre elles, ces deux programmes ont toujours fonctionné indépendamment l'un de l'autre. Pour atteindre ses buts stratégiques, le CST a l'intention d'exploiter les synergies créées par le rapprochement des deux programmes. En examinant les vulnérabilités des systèmes de communication et d'information ensemble, les experts du SIGINT et de la STI mettent maintenant leur savoir en commun pour repérer les menaces visant les systèmes canadiens, ainsi que les occasions de recueillir des renseignements sur l'étranger.

En juin 2000, le chef du CST m'a présenté un exposé sur ce sujet. Par la suite, mon bureau a examiné la stratégie dans le détail avec la haute direction de l'organisme. Je ne pense pas que cela modifiera fondamentalement la façon dont j'examine les activités du CST, car je continuerai d'en juger la légalité. Entre-temps, j'ai exprimé mon appui pour cette entreprise.

EXAMEN DU CST

Le rôle du commissaire

Mon mandat d'examiner les activités du CST et de faire rapport au ministre de la Défense nationale est exposé dans un décret (voir annexe A).

Chaque année, mon bureau recense des secteurs des activités du CST où, de prime abord, on pourrait présumer qu'il se pose des questions de

légalité. Il effectue ensuite, avec mon autorisation, des examens systématiques de ces activités. Je communique les résultats de ces examens au ministre de la Défense nationale sous la forme de rapports classifiés. La production d'un rapport classifié n'indique pas que j'ai découvert un cas d'illégalité. Elle indique plutôt que le rapport renferme des renseignements de nature délicate qui nécessitent cette classification.

Les travaux de recherche et de préparation qu'exigent mes rapports au ministre représentent le gros du travail de mon bureau et me procurent une information détaillée touchant divers aspects des activités du CST.

J'ai examiné les autorisations en vertu desquelles le CST recueille des renseignements sur l'étranger au nom du gouvernement du Canada, ainsi que son mandat de protéger la sécurité des technologies de l'information du gouvernement. Et j'examine régulièrement ses politiques, directives et pratiques afin de m'assurer qu'elles contribuent à la légalité de ses activités et à la protection de la vie privée des Canadiens.

Mes examens ont porté, entre autres, sur la façon dont le CST fournit des rapports de renseignement à ses clients, et sur la réception de renseignements de ses partenaires des Secondes Parties. Je surveille régulièrement les activités opérationnelles de l'organisme, ainsi que les circonstances ayant mené à des enquêtes sur la sécurité interne.

On trouvera à l'annexe B la liste des rapports classifiés que j'ai communiqués au ministre depuis ma nomination, en 1996.

Activités de l'année 2000-2001

Produits du renseignement sur l'étranger

Au cours de l'année écoulée, j'ai continué à examiner les activités du CST sous l'angle de leurs rapports avec le cycle du renseignement, ainsi qu'avec le traitement et la production des produits du renseignement. Comme je le mentionnais dans mon dernier rapport annuel, le CST examine quotidiennement les transmissions brutes qu'il reçoit de nombreuses sources et en évalue la valeur sur le plan du renseignement étranger par rapport aux priorités du gouvernement. Il communique ensuite les résultats de ce travail à ses clients du gouvernement sous la forme de produits du renseignement.

L'année passée, j'ai examiné les politiques et les pratiques de traitement liées à la réception et à la conservation des transmissions de renseignements sur l'étranger. Je me suis penché sur la façon dont le CST reconnaît les questions présentant un intérêt en matière de renseignement dans les transmissions brutes qu'il reçoit, et sur les pratiques liées à leur conservation et à leur diffusion subséquente sous la forme de rapports de renseignement. Et, comme je le fais d'habitude, j'ai examiné les politiques et les pratiques du CST qui, dans ce cycle d'activités, visent expressément à sauvegarder la vie privée des Canadiens.

Gestion de l'information

J'ai en outre examiné les politiques de gestion de l'information du CST à la lumière de la *Loi sur les archives nationales du Canada* ainsi que de la politique et des lignes directrices du Conseil du Trésor touchant la gestion des fonds de renseignements.

Les ministères et organismes sont tenus d'établir des autorisations de disposition de documents pour leurs fonds de renseignements opérationnels et administratifs. Ces autorisations leur permettent de se débarrasser de certains fonds de renseignements et les obligent à transmettre aux Archives nationales d'autres fonds présentant un intérêt archivistique, pour y être conservés.

J'ai constaté que ces autorisations ne constituent pas une obligation de détruire des documents et qu'elles ne donnent aucune indication quant au moment où ceux-ci doivent être détruits. Par ailleurs, elles ne prévoient ni n'autorisent de périodes de conservation des documents. Les périodes de conservation et d'élimination sont déterminées par le ministre responsable de l'institution et doivent, bien entendu, être conformes à toute autre loi applicable.

J'ai acquis la conviction que les politiques du CST se conforment aux exigences des lois et des politiques relatives à la gestion des fonds de renseignements du gouvernement. Je recommande toutefois que le CST s'occupe en priorité de compléter ses calendriers de conservation et d'élimination.

Pouvoirs en matière de politiques

Dans mon rapport annuel de 1998-1999, je signalais mon intention d'examiner le nouveau cadre de pouvoirs, de responsabilité et de coordination touchant les politiques, que le CST avait adopté peu auparavant. Je m'intéressais plus particulièrement à deux des objectifs de ce cadre, soit déterminer le palier approprié pour différentes politiques, et procurer un niveau souhaitable de souplesse opérationnelle pour les activités quotidiennes.

Au cours de l'année passée, j'ai examiné le nouveau cadre, et je l'ai trouvé bien conçu et judicieux. Il faudra cependant du temps pour y adapter toutes les politiques de l'organisme. S'il subsiste certaines lacunes, le CST dispose de politiques pour ses besoins essentiels, et le nouveau système devrait répondre à mon souci antérieur de trouver les politiques au bon palier de l'organisation et de les voir approuvées au niveau approprié.

Au cours de l'année à l'étude, j'ai appris avec plaisir que des fonctionnaires avaient entamé des entretiens dans le but de faire communiquer les politiques internes de base au CST sous la forme

d'ordres du ministre. J'applaudis cette initiative, car elle renforcera les liens de responsabilité entre le CST et le ministre de la Défense nationale, qui est comptable de l'organisme devant le Parlement.

Autres activités

Mon mandat m'autorise à enquêter sur les plaintes déposées par des Canadiens ou des résidents permanents du Canada au sujet des activités du CST. Des demandes de renseignements officieuses ont été faites en 2000-2001, mais aucune n'a abouti à une plainte officielle.

Au cours de l'année dernière, mon bureau a entretenu des contacts officieux au sein de la communauté de la sécurité et du renseignement. Nous avons été particulièrement heureux d'accueillir l'inspecteur général de l'Afrique du Sud pendant sa tournée de l'automne 2000 en Amérique du Nord. J'envisage par ailleurs avec plaisir de renouer connaissance avec mes homologues d'autres pays lors de la prochaine conférence des organismes d'examen, à Washington, en octobre 2001.

Constatations faites en 2000-2001

Je suis convaincu que, au cours de la période à l'examen, le CST a agi conformément à la loi dans l'exécution de son mandat, et qu'il n'a pas ciblé les communications de citoyens ni de résidents permanents du Canada. Je fais cette affirmation en me fondant sur l'examen approfondi de ses activités effectué pendant l'année.

Mon mandat m'oblige à informer le ministre de la Défense nationale et le procureur général du Canada de toute activité du CST qui, à mon sens, n'est peut-être pas conforme à la loi. Je n'ai pas eu à faire cela jusqu'ici. Le CST est conscient des limites qui lui sont imposées, il reçoit les avis de conseillers juridiques affectés auprès de l'organisme par le ministère de la Justice, et il dispose de politiques et de procédures destinées à promouvoir la légalité. Ces mesures se sont révélées efficaces.

Personnel et budget

Le budget qui m'avait été alloué pour l'année financière 2000-2001 était de 648 800 $. Je suis en mesure de signaler qu'il a bien suffi à couvrir les dépenses réelles engagées.

Mon bureau se compose toujours de deux employés à plein temps et de plusieurs spécialistes dont je retiens les services par contrat. À l'heure actuelle, cinq personnes effectuent des travaux spécialisés selon cette formule, et toutes possèdent l'autorisation sécuritaire requise. Cette façon de procéder m'assure la continuité et la souplesse voulues pour obtenir les compétences dont j'ai besoin afin d'examiner efficacement les activités du CST.

COUP D'ŒIL SUR L'AVENIR

Sauvegarder la vie privée des Canadiens

Comme je l'ai déjà fait remarquer, la technologie de collecte de renseignements sur l'étranger du CST doit se perfectionner constamment pour suivre le rythme du progrès des technologies de communication. Malgré la plus grande efficacité des nouvelles technologies, il reste probable que le CST recevra involontairement de petites quantités de communications canadiennes. De plus, chaque nouveau système ou technique de collecte mis en service semble comporter cette possibilité. Cependant, le CST est bien conscient du fait qu'il doit constamment étendre ses moyens d'écarter les communications canadiennes, ou risquer d'agir illégalement s'il ne fait pas tous ses efforts dans ce sens.

À cet égard, j'ai informé le CST que, en plus de mes autres activités d'examen, je chercherai à m'assurer qu'il utilise toutes les technologies nouvelles pour veiller à sauvegarder la vie privée des Canadiens.

CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

C.P. 1999-1048
8 juin 1999

Sur recommandation du ministre de la Défense nationale et en vertu de la partie II de la *Loi sur les enquêtes*, Son Excellence le Gouverneur général en conseil autorise le ministre de la Défense nationale (le « ministre ») :

a) à reconduire l'honorable Claude Bisson, de Montréal (Québec), dans ses fonctions de commissaire du Centre de la sécurité des télécommunications (le « CST ») pour une période de trois ans pendant laquelle il examinera les activités du CST et s'assurera qu'elles sont conformes à la loi;

b) à autoriser le commissaire à entreprendre cet examen de sa propre initiative ou à la requête du ministre;

c) à autoriser le commissaire à instruire toute plainte concernant la légalité des activités du CST que pourrait déposer un citoyen canadien ou un résident permanent du Canada;

d) à autoriser le commissaire à ne pas instruire une plainte lorsque, de l'avis de celui-ci, il existe d'autres recours légaux;

e) à autoriser expressément le commissaire à informer toute personne ayant déposé une plainte des résultats de l'enquête qui a été effectuée, en prenant soin de ne divulguer aucun renseignement confidentiel à cette personne;

f) à enjoindre au commissaire de signaler au ministre et au procureur général du Canada toute activité du CST qu'il estime ne pas être conforme à la loi;

.../2

g) à enjoindre au commissaire de présenter au ministre, une fois l'an et dans les deux langues officielles, un rapport sur ses activités et ses constatations qui ne sont pas de nature confidentielle, le rapport devant être déposé par le ministre au Parlement;

h) à autoriser le commissaire à présenter au ministre, et ce à tout moment jugé opportun par le commissaire, un rapport contenant des renseignements confidentiels;

i) à enjoindre au commissaire, avant la présentation de tout rapport au ministre, de consulter le sous-secrétaire du Cabinet (Sécurité et renseignement) au Bureau du Conseil privé pour s'assurer que toutes les exigences relatives à la sécurité sont respectées, y compris la confidentialité des sources et la protection des renseignements obtenus de pays étrangers;

j) à exiger que le commissaire et toutes les personnes engagées pour son compte prononcent un serment de discrétion et se conforment à toutes les exigences du gouvernement en matière de sécurité;

k) à autoriser le commissaire à retenir les services de toute personne dont il juge avoir besoin pour l'assister dans ses fonctions, aux taux de rémunération et d'indemnisation que peut approuver le Conseil du Trésor;

.../3

l) à fixer la rémunération du commissaire au taux journalier établi dans l'annexe ci-jointe, lequel se situe entre 400 $ et 500 $;

m) à autoriser le remboursement des frais de transport et de séjour raisonnables engagés par le commissaire lorsque l'exercice de ses fonctions l'amène à s'éloigner de son lieu de résidence habituel, conformément aux directives du Conseil du Trésor concernant les déplacements;

à compter du 19 juin 1999.

CERTIFIED TO BE A TRUE COPY–COPIE CERTIFIÉE CONFORME

CLERK OF THE PRIVY COUNCIL–LE GREFFIER DU CONSEIL PRIVÉ

Rapports classifiés, 1996-2001

Classified Report to the Minister - 3 mars 1997 (TRÈS SECRET)

Classified Report to the Minister
- Operational Policies with Lawfulness Implications - 6 février 1998 - (SECRET)

Classified Report to the Minister
- CSE's Activities under *** - 5 mars 1998 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- Internal Investigations and Complaints - 10 mars 1998 (SECRET)

Classified Report to the Minister
- CSE's activities under *** - 10 décembre 1998 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- On controlling communications security (COMSEC) material - 6 mai 1999 (TRÈS SECRET)

Classified Report to the Minister
- How We Test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) - 14 juin 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- A Study of the *** Collection Program - 19 novembre 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- On *** - 8 décembre 1999 (TRÈS SECRET - COMINT)

Classified Report to the Minister
- A Study of the *** Reporting Process - an overview (Phase I) - 8 décembre 1999 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A Study of Selection and *** - an overview - 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's Operational Support Activities Under *** - follow-up - 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- Internal Investigations and Complaints - follow-up - 10 mai 2000 (SECRET)

Classified Report to the Minister
- On findings of an external review of CSE's ITS Program - 15 juin 2000 (SECRET)

Classified Report to the Minister
- CSE's Policy System Review - 14 septembre 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase II *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase III *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)